

Section VI

HIPAA: Policies, Procedures and Forms

**PROVIDER MANUAL
FOR
COMMUNITY MENTAL HEALTH,
DEVELOPMENTAL DISABILITIES AND
ADDICTIVE DISEASES
PROVIDERS
FOR
THE DIVISION OF MENTAL HEALTH,
DEVELOPMENTAL DISABILITIES AND
ADDICTIVE DISEASES**



JULY 2006

CONFIDENTIALITY

I. Legal References

21 CFR § 1175, O.C.G.A. §§ 24-9-21; 26-5-17; 37-3-166; 37-4-125; 37-7-166; 37-2-1.2; 43-39-16.

To respect and acknowledge the privacy and confidentiality of consumers is the responsibility of all who participate in the delivery of services to the disabled. Confidential consumer information contained in records, charts, documents or other forms of recordation may be released only on a need to know basis to persons authorized by law or upon written consent of the consumer. Furthermore, it is advisable that consumer information not be discussed openly, other than is necessary to benefit the consumer, and only among duly authorized staff or others clearly involved in the care of the consumer.

II. Confidential Information

Need to know information includes, but is not limited to, information used to:

- A. Determine eligibility
- B. Provide treatment for, or contribute to, the diagnosis of any medical or psychological illness, injury, or condition
- C. Assess financial liability
- D. Pay any financial obligations
- E. Initiate or further any investigatory, regulatory, or enforcement purpose
- F. Provide service

III. Considerations

To meet the needs of consumer's in an efficient, effective way, and to accomplish the goal of simplifying access to services, contractors may share consumer information on a need to know basis across provider/program lines unless prohibited by state or federal law. The disclosure of consumer information shall be guided as follows:

- A. Contractors shall respect and acknowledge the privacy rights of consumers.
- B. Only those persons with proper authorization may access confidential consumer information.
- C. Consumers shall be informed that information and records may be shared with authorized persons.
- D. Contractors shall be responsible for handling and safeguarding consumer records to protect their confidentiality.

IV. Sharing Consumer Information

- A. Contractors may share consumer information within its organization on a need to know basis in furtherance of consumer's treatment or programmatic goals.
- B. Policies and procedures should be established for determining which employees shall have access to different types of consumer information.
- C. Contractors should develop a procedure for handling requests for consumer information from outside its organization.

V. Clinical Records

Perhaps the greatest source of confidential consumer information is the consumer's clinical records. These records are afforded specific protections under the law and must be handled in a manner designed to meet the law's requirements. Providers are urged to consult O.C.G.A. § 37-3-166 (MH); 37-4-125 (MR) and 37-7-166 (SA), to determine when such clinical information may be disclosed. A thorough reading of the applicable statute and/or legal consultation is urged when there is uncertainty regarding the disclosure of consumer information to anyone not directly involved in their treatment.

VI. Unauthorized Disclosure of Consumer Information

Georgia Law and Federal Regulations protect the consumer's right to confidentiality. Any violation of the consumer's right to confidentiality may subject the party or parties responsible for the unauthorized disclosure to statutory penalties and/or civil action.

Policy Subject: Protection of Individually Identifiable Health Information – Compliance with HIPAA Privacy Rules

REFERENCE: 45 CFR Parts 160 and 164; DHR HIPAA Policies 1.0, 2.0, 3.0, 4.0, 5.0, 6.0, 7.0, 8.0, 9.0, 10.0, 11.0, 12.0, 15.0, 16.0, and 20.0.

I. POLICY STATEMENT

It is the policy of the Division of Mental Health, Developmental Disabilities and Addictive Diseases (DMHDDAD) to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and related Department of Human Resources (DHR) policies by establishing the needed procedures and related protocols. HIPAA does not supercede or negate more stringent federal and state laws, rules and regulations.

II. APPLICABILITY

The DHR is a covered entity under HIPAA and the Privacy Rule, and the DMHDDAD is covered as a part of the Department. This policy is therefore applicable to any entity that is a part of the division, including the state office, regional offices, state operated DMHDDAD hospitals and any state operated community programs. All employees, agents, trainees, volunteers and contractors of the DMHDDAD shall abide by the DMHDDAD and DHR policies and all federal, state and local laws regarding the disclosure and use of protected health information. DMHDDAD service providers who are under contract or have a letter of agreement with the DHR through the DMHDDAD and its Regional Offices are business associates of the DMHDDAD (see definition of business associate below) and must comply with applicable provisions of the Privacy Rule.

III. DEFINITIONS

- A.** Authorization – Permission by a consumer or a person legally authorized to consent on his/her behalf, for the release or use of protected health information.
- B.** Business Associate - A person or entity who is not a member of the covered entity's work force and who, on behalf of the covered entity, performs or assists in the performance of a function or activity involving the use of individually identifiable health information.
- C.** Covered Entity – A health care provider, health plan, or health care clearinghouse that transmits any health information in electronic form in connection with a HIPAA transaction; Georgia DHR is a covered entity.

- D.** De-identified Information – Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.
- E.** Disclosure – Release, transfer, provision of access to, or divulging in any other manner, information by an entity to persons or organizations outside of that entity.
- F.** Accounting of disclosures – A history of when and to whom disclosures of protected health information are made for purposes other than treatment, payment, and health care operations.
- G.** Health and Human Services (HHS) – The federal government department that has overall responsibility for implementing HIPAA.
- H.** Health Insurance Portability and Accountability Act of 1996 (HIPAA) – A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care consumers, providers, payers, and employers; and to specify the types of measures required to protect the security and privacy of personally identifiable health care information. Also known as the Kennedy-Kassebaum Bill, the Kassebaum-Kennedy Bill, K2, or Public Law 104-191.
- I.** Individually Identifiable Health Information (IIHI) – Any information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, and identifies the individual; or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. IIHI contains some or all of the following elements:
1. Name
 2. All Address Information
 3. E-Mail Addresses
 4. Dates (except year)
 5. Social Security Number
 6. Medical Record Numbers
 7. Health Plan Beneficiary Numbers
 8. Account Numbers
 9. Certificate Numbers
 10. License Numbers
 11. Device Identifiers
 12. URLs
 13. IP Addresses
 14. Facial Photographs
 15. Biometric Identifiers
 16. The initial three digits of the zip code, unless the geographic unit formed by combining all zip codes with the initial three digits contains more than 20,000 people or the initial three digits of all geographic units with fewer than 20,000 people is changed to 000

17. Any other unique identifying number, characteristic, or code
- J.** Minimum Necessary – When using or disclosing protected health information or when requesting PHI, the process of making reasonable effort to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
 - K.** Notice of Privacy Practice – A notice that provides a clear explanation of the covered entity's privacy practices and the privacy rights of consumers regarding their personal health information.
 - L.** Patient-Identifiable Data – Information that relates to a person's physical or mental health, and that contains enough information to identify the particular individual reflected in the information.
 - M.** Person legally authorized to sign: A person authorized by law to give authorization for disclosure of an individual's protected health information. These persons include, for minors, the parent, the court-appointed guardian or the court-appointed custodian; for adults, the court-appointed guardian of the person.
 - N.** Privacy – HIPAA regulations protect an individual's right to the privacy of his or her medical information to keep it from falling into the hands of people who would use it for commercial advantage, personal gain or malicious harm. The HIPAA privacy regulations require providers to obtain a signed authorization to use or disclose PHI.
 - O.** Privacy Coordinator – The individual designated by the Division (DMHDDAD) with responsibility for obtaining and maintaining a working knowledge of the Department's and Division's privacy and security policies and procedures and of the Privacy Rule to respond to HIPAA-related inquiries arising within the Division, provide information regarding the complaint process and maintain adequate documentation of these activities.
 - P.** Privacy Officer – The individual designated by the Department (Georgia DHR) with responsibility for obtaining and maintaining a working knowledge of the Department's privacy and security policies and procedures and of the Privacy Rule to respond to HIPAA-related inquiries arising within the Department, provide information regarding the complaint process and maintain adequate documentation of these activities. Also has responsibility for coordination of Privacy Coordinators and for certain HIPAA-related reporting.
 - Q.** Privacy Rule – Standards for Privacy of Individually Identifiable Health Information, which implements the privacy requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45 CFR parts 160 and 164.
 - R.** Protected Health Information (PHI) – All individually identifiable health information (e.g., name, Social Security number, medical record number, etc.) transmitted or maintained by a covered entity, regardless of form.
 - S.** Workforce – Under HIPAA, this means employees, volunteers, trainees, and other persons under the direct control of a covered entity, whether or not they are paid by the covered entity.

IV. PROCEDURES

- A.** The DMHDDAD shall have a method to allow individuals to exercise their right to request that DMHDDAD amend PHI or a record about the individual in a

designated record set used in whole or in part to make decisions about the individual, for as long as DMHDDAD maintains the PHI in the designated record set.

- B.** DMHDDAD shall develop and communicate to individuals a process for filing complaints about the division's privacy practices or perceived violations of the Privacy Rule standards and implementation specifications. Such process shall include expectations regarding cooperation with investigations regarding complaints and for reporting as required for compliance reviews.
- C.** DMHDDAD shall document HIPAA privacy policies, procedures and protocols, either on paper or in electronic form. Any change to a policy, procedure or protocol shall be documented. In addition to policies, procedures and protocols, any correspondence or other documents pertaining to the accounting of disclosures by DMHDDAD shall be documented and maintained on file for six years, or longer if required under other applicable laws, regulations or policies.
- D.** DMHDDAD shall implement policies, procedures and protocol that are designed to comply with Privacy Rule standards and all implementation specifications for PHI. Policies, procedures and protocol shall be reasonably designed and take into account the size and type of activities that relate to PHI undertaken by DMHDDAD. These policies, procedures and protocols shall:

 - 1. Restrict access and use based on specific roles of members of DMHDDAD's workforce;
 - 2. Establish criteria to limit routing disclosures to minimum necessary to achieve the purpose of the disclosure;
 - 3. Limit requests to other covered entities to what is reasonably necessary for the particular use or disclosure; and
 - 4. Control when staff requests or discloses the entire medical record. There must be specific justification of the need for the entire medical record.
- E.** DMHDDAD shall mitigate, to the extent practicable, any harmful effect that is known of a use of disclosure of PHI by DMHDDAD or a business associate, in violation of DMHDDAD policies, procedures and protocols or the requirements of the Privacy Rule.
- F.** DMHDDAD shall permit an individual to request a restriction of disclosures.

 - 1. DMHDDAD does not have to agree with the restriction.
 - 2. If DMHDDAD agrees to the restriction, both DMHDDAD and its business associates shall honor the restriction, until DMHDDAD or the individual terminates the restriction.
 - 3. If the individual terminates the restriction, DMHDDAD may use and disclose PHI as permitted under the Privacy Rule. If DMHDDAD terminates the restriction without the individual's agreement, it may only terminate the restriction with respect to PHI it creates or receives after it informs the individual of the termination.

4. In the case of an emergency treatment situation, DMHDDAD is allowed to release PHI to the health care provider. DMHDDAD shall request the provider not further use or disclose the PHI.
 5. DMHDDAD shall document the restriction to which DMHDDAD and the individual have mutually agreed.
- G.** DMHDDAD shall develop physical safeguard standards and access controls for PHI it collects and maintains.
- H.** DMHDDAD shall have sanction policies, procedures or protocols documented so that employees are aware of what actions are prohibited and punishable. Such sanctions shall comply with the HIPAA Privacy Rule standard for sanctions against members of DMHDDAD's workforce who fail to comply with its privacy policies, procedures and protocols. Appropriate sanctions shall be imposed for violations of DMHDDAD's privacy policies and procedures, or related protocols, standards or directives. Sanctions that may be imposed by DHR are cumulative of those that may be imposed by statute or regulation.
- I.** DMHDDAD shall train all current and newly hired members of its workforce on its privacy policies, procedures and protocols as necessary and appropriate for them to carry out their functions within DMHDDAD, according to a training plan for HIPAA awareness.
- J.** DMHDDAD shall obtain from business associates reasonable assurances that they will appropriately safeguard PHI disclosed by DMHDDAD and that agents, employees and subcontractors of the business associates agree to the same conditions applicable to the business associates with respect to such information. DMHDDAD shall include HIPAA compliance requirements in contracts, other written agreements and expressions of understanding, and purchase orders with business associates to whom DMHDDAD discloses PHI.
- K.** DMHDDAD shall have a written authorization from an individual before using or disclosing PHI for any purpose not otherwise permitted or allowed by the Privacy Rule.
- L.** DMHDDAD shall keep an accounting of when and to whom disclosures of PHI are made for purposes other than treatment, payment and health care operations, and shall be able to give an accounting of those disclosures to an individual, if requested. Authorizations from an individual to DMHDDAD are included in the information that is to be tracked and accounted for. A disclosure of PHI that does not require an authorization may, in some cases, have a tracking and accounting requirement.
- M.** DMHDDAD shall establish a means for an individual to access and inspect his/her PHI in a designated record set for as long as DMHDDAD maintains the PHI in the designated record set.

- N.** DMHDDAD will establish and implement minimum necessary requirements for uses and disclosures of PHI. DMHDDAD shall make reasonable efforts to limit PHI used, disclosed or requested from another covered entity to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
- O.** DMHDDAD shall provide adequate notice to individuals of the uses and disclosures of PHI it may make by providing a Notice of Privacy Practices to persons seeking or receiving services. DMHDDAD shall document its compliance with the notice requirements by retaining copies of the notices it issues.
- P.** If DHR decides in the future to permit the use or disclosure of health information without authorization to a business associate for fund raising purposes, DMHDDAD shall limit such use or disclosure to demographic information about an individual and dates on which health care was provided to the individual. In such event, all fundraising materials shall include a description of the manner in which the individual may opt out of receiving further fundraising communications, and the Division shall take reasonable steps to ensure that such communications are no longer sent to individuals who choose to opt out.
- Q.** DMHDDAD shall establish standards relating to uses and disclosures, and de-identification and re-identification of PHI it creates, collects and maintains.
- R.** DMHDDAD shall establish standards relating to uses and disclosures of PHI for marketing purposes in the event DMHDDAD should undertake to engage in marketing after the Privacy Rule becomes effective. As of April 14, 2003, DMHDDAD shall not engage in marketing activities within the meaning of the Privacy Rule, pursuant to the policy of DHR.
- S.** DMHDDAD shall allow authorized revisions of these privacy policies and procedures in response to changes in administrative, operating or programmatic requirements. The DHR Privacy Officer must approve any and all revisions.
- T.** DMHDDAD shall adopt supplemental internal privacy policies, procedures or protocols where necessary to meet the requirements of specific programs, activities, or federal or state laws and regulations. Such policies, procedures or protocols shall conform to those of the Department and the Privacy Rule and are subject to review by the DHR Privacy Officer.
- U.** DMHDDAD shall examine its policies, procedures and protocol on an ongoing basis and as necessary revise these to meet requirements of applicable laws and regulations, including the Privacy Rule.
- V.** DMHDDAD shall designate a Privacy Coordinator as well as a contact person to be responsible for complaints and to provide privacy practice information. The Privacy Coordinator shall obtain and maintain an adequate working knowledge of DHR's and DMHDDAD's privacy and security policies, procedures and protocols and of the Privacy Rule to respond to HIPAA related inquiries arising within DMHDDAD, provide information regarding the complaint process and maintain

adequate documentation of these activities. The Privacy Coordinator shall submit reports of privacy related activities periodically to the DHR Privacy Officer and to the Commissioner of the Department upon request.

The Division may appoint Associate Privacy Coordinators at the regional, institutional or other administrative level. Associate Privacy Coordinators shall obtain and maintain a working knowledge of the DMHDDAD's privacy and security policies, procedures and protocols and of the Privacy Rule equivalent to that required of DMHDDAD. Associate Privacy Coordinators must submit monthly summaries of their privacy-related activities to the Privacy Coordinator.

- W.** Violation of Division and/or Department privacy policies, procedures and protocols shall be communicated to the DMHDDAD Privacy Coordinator. Violation reports shall include the date of discovery, nature of the violation, a description of any actions taken within the work unit to mitigate harmful effects of the violation and prevent recurrence, and if known, the name and title of the violator, information about the violator's intent and information on previous similar occurrences. Violation reports shall be in writing for documentation purposes, and may be submitted by mail, as attachments to e-mail, by facsimile or other electronic means.

**Sections/Office/Unit Responsible for
Policy Development/Review:**
Legal and Risk Management

Approved:
Karl Schwarzkopf, Director
April 8, 2003

Instructions for HIPAA Privacy Rule Forms

Pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), covered entities must maintain, and in some cases provide to individuals copies of, a Notice of Privacy Practices, Authorization(s) for Use or Disclosure of Protected Health Information, and Business Associate Agreements. This packet includes samples of these three documents that you may use as guidance in complying with the Act, as well as the following instructions for each document. However, THESE SAMPLES ARE NOT TO BE CONSTRUED AS LEGAL ADVICE AND NO REPRESENTATION OF LEGAL SUFFICIENCY FOR PURPOSES OF YOUR ENTITY’S COMPLIANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (“THE ACT”) IS BEING PROVIDED. IT IS YOUR RESPONSIBILITY TO ENSURE THAT YOUR ENTITY COMPLIES WITH THE ACT.

Notice of Privacy Practices

Providers must immediately begin to give to all current and new consumers a copy of this form, and ask them to read and sign it. If applicable, the consumer’s parent (for minors) or guardian may sign the form on the consumer’s behalf. The provider must give a copy of the notice to the person who signed it. If the consumer or parent/guardian declines to sign the form, the provider should still give a copy of the form to the consumer or parent/guardian. Providers must ensure that a copy of the form is maintained in the consumer’s clinical record.

Every consumer is entitled to a copy of this form upon request. Therefore, providers should keep a supply of the form available. Parents and guardians may also request a copy.

The provider must ensure that this notice is also posted at all times in a prominent location where it is reasonable to expect individuals who are seeking or receiving services to be able to read the notice.

Authorization for Use or Disclosure of Protected Health Information

This form replaces any form, including **DHR Form 5459**, previously used for the consumer, parent (for minors) or guardian to sign in order to authorize disclosure of the consumer’s protected health information. Please immediately destroy all blank copies of other authorization forms that you may have. Providers must begin immediately to use this form to obtain any new authorization(s) for the use or disclosure of information regarding all current and new consumers. Providers must maintain a copy of each fully completed and signed form in the consumer’s clinical record. A provider may choose to modify this form, for instance, by adding spaces for the consumer’s name and identifying information (kardex type data), or to add the name and contact information of the provider.

Business Associate Agreement

Contracted providers of DHR are Business Associates of DHR as defined in the HIPAA Privacy Rule. As such, they must sign a Business Associate Agreement with DHR. Business Associate language will be incorporated into the contract template language for all DHR FY '04 contracts.

Providers, as Business Associates of DHR, are required to ensure that their agents and/or subcontractors comply with all Privacy Rule requirements that are applicable to the Provider. Providers will, therefore, enter into Business Associate Agreements with their agents and/or subcontractors who have access to protected health information of individuals served under the provider's contract(s) with DHR.

Providers must retain copies of all Business Associate Agreements for as long as they do business with the agent and/or subcontractor, or for six (6) years, whichever is longer. The Provider will give DHR access to each of its Business Associate Agreements upon request.

NOTE: For written contracts existing as of October 15, 2002, and not renewed or modified by April 14, 2003, the Provider has until April 14, 2004, to enter a Business Associate Agreement with agents and/or subcontractors. **In all other cases**, Providers must obtain signed agreements with all their applicable agents and/or subcontractors **by April 14, 2003**.

Part V

HIPAA APPENDICES

Georgia Department of Human Resources Division of Mental Health, Developmental Disabilities and Addictive Diseases	PROTOCOL NO: 3.200-01
	ORIGINAL EFFECTIVE DATE:
PROTOCOL SUBJECT: Individual Rights Regarding Protected Health Information	REVISED EFFECTIVE DATE: N/A
	PAGE 1 OF 7

PROTOCOL

Pursuant to the Health Insurance Portability and Accountability Act (HIPAA), an individual has the right to inspect and/or obtain a copy of his/her Protected Health Information (PHI), to request restriction of the uses and disclosures of his/her PHI, to request alternative means or location of communications of PHI, to correct or amend his/her PHI, and to receive an accounting of disclosures of PHI.

This protocol applies to all state owned and operated programs, and to all providers contracting with the Department through the regions. Each such entity is referred to in this protocol as the “record holder.”

I. Access to Protected Health Information (PHI)

A. Individual Access to One’s Own PHI.

1. A request for access to PHI must be acted upon within thirty-30-days of receipt; there may be one (1) extension for an additional thirty-30-days.
2. Reasonable fees may be charged for access to PHI based on actual cost, if the recipient agrees to the fees in advance.
3. The designated record sets that are subject to access by individuals must be documented. “Designated record set” includes the individual’s clinical record and billing records.
4. The titles of persons or offices responsible for receiving and processing requests for access to PHI must be documented.
5. Parents have the right to access and control health information about their minor children, with the following exceptions:
 - a) The fact that a minor has applied for substance abuse treatment may be disclosed to the parent, guardian, or court-ordered custodian only if:
 1. the minor gives written authorization
OR
 2. the clinical director of the program documents his/her finding that the minor child lacks capacity, either due to extreme youth or mental or physical condition, to make a rational decision on whether to authorize disclosure of substance abuse PHI.
 - b) Facts relevant to reducing a threat to the life or physical well-being of a minor applicant for substance abuse services or any other individual may be disclosed to the parent, guardian, or court-ordered legal custodian if, in the written opinion of the clinical director,
 1. the minor child lacks capacity to make a rational decision, either due to extreme youth or mental or physical condition, on whether to authorize disclosure of substance abuse PHI to the parent, guardian, or court-ordered legal custodian, AND
 2. the applicant’s situation poses a substantial threat to the life or physical well being of him/herself or any other person, which may be reduced by communicating relevant facts to the minor’s parent, guardian, or court-ordered custodian.
 - (c) For a minor who is undergoing substance abuse treatment by consent of his/her parent, guardian, or court-ordered custodian, disclosure of substance abuse PHI requires the consent of both the minor child and the parent/guardian.

6. All documentation related to requests for access to PHI must be retained for a minimum of six (6) years.

B. Denial of an Individual's Access to His/Her Own PHI

1. Denials of requests for access must be in writing.

2. Access to an individual's PHI may be denied without providing the individual an opportunity for review in the following cases:

- a. Psychotherapy notes. "Psychotherapy notes" for purposes of this protocol and the Privacy Rule, is defined to mean notes recorded in any medium by a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.
- b. Information compiled in anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
- c. Information created or obtained in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress.

3. An individual's access to his/her own PHI may also be denied in the following circumstances, provided the individual is given the right to have the denial reviewed:

- a) The chief medical officer or the individual's treating physician has determined, in the exercise of professional judgment, that the access requested is detrimental to the individual's physical or mental health. This restriction applies only to individuals who are currently being treated by the facility or program from which they are requesting records.
- b) The PHI makes reference to another person (unless the other person is a health care provider) and the chief medical officer or the individual's treating physician has determined, in the exercise of professional judgment, that the access requested is likely to cause substantial harm to such other person. However, names and PHI of other individuals who are patients or consumers will always be redacted, and this restriction is not subject to review.

- c) The request for access is made by the parent of a minor, court-ordered custodian of a minor, guardian of the person of an individual, or a legal representative of the individual's estate, and the chief medical officer or the individual's treating physician has determined, in the exercise of professional judgment, that the provision of access to the requestor is reasonably likely to cause substantial harm to the individual or another person.
- 4 .If a request to access PHI is denied, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the record holder to act as a reviewing official and who did not participate in the original decision to deny access; DMHDDAD must abide by the reviewing official's decision as final.
- 5 If an individual's request to access PHI is denied, the denial must comply with the requirements of the Privacy Rule, which include:
- a. Making other information accessible.
 - b. Providing a timely, written denial in plain language that must include the basis for the denial, a statement of the individual's right to have the denial reviewed (if applicable) and a description of the procedures for complaints to the record holder, DMHDDAD, DHR or the Secretary of DHHS.
 - c. If the record holder does not maintain the PHI for which access has been requested, but knows where the requested PHI is maintained, the record holder must inform the individual where to direct the request for access.
 - d. All requests for review must be promptly referred to the designated reviewing official; the designated official must make a determination within a reasonable period of time.
 - e. All documentation related to denial of requests for access to PHI must be retained for a minimum of six (6) years.

II. Individual's Restriction of Access by Others to His/Her Protected Health Information (PHI)

- A. Individuals must be permitted to request the restriction of use and disclosure of the individual's PHI.
- 1. The record holder does not have to agree to the request for restriction.
 - 2. If the record holder agrees to the request for restriction, both the record holder, DMHDDAD and their business associates shall honor the restriction, until the record holder or the individual requesting the restriction terminates the restriction.
 - 3. If the individual terminates the restriction, the record holder may use and disclose PHI as permitted under the Privacy Rule, applicable law and regulations, and Division policies; if the record holder terminates the restriction without the individual's agreement, it may only terminate the restriction with respect to PHI that it creates or receives after it informs the individual of the termination.
 - 4. In the case of an emergency treatment situation, the record holder is allowed to release PHI to the health care provider and the health care provider will be requested to not further use or disclose the PHI.
 - 5. The record holder shall document the restriction to which it and the individual have mutually agreed in the individual's clinical record.
 - 6. All documentation related to restricting access to PHI must be retained for a minimum of six (6) years.

III. Individuals must be permitted to request to receive communications of PHI from the record holder by alternative means or alternative locations.

- A. The record holder must accommodate reasonable requests.
- B. The record holder may require that the individual put the request in writing.
- C. The record holder may condition reasonable accommodation of the request on:
 - 1. When appropriate, information as to how payment, if any, will be handled, and
 - 2. Specification of an alternative address or other method of contact.

- D. The record holder may not require an explanation from the individual for the basis of the request.

IV. Amending Protected Health Information (PHI)

- A. Individuals may request the amendment of their PHI maintained in the designated record set (the individual's clinical record or billing records).
 1. Requests for PHI amendments must be made in writing, and must include a reason to support the requested amendment; individuals must be informed in advance of these requirements.
 2. Requests for a PHI amendment must be acted upon no later than 5 days following receipt of the request.
 3. The record holder must respond to the request by providing the individual with a written acknowledgment, if the request includes sufficient information to permit a reply to be mailed to the individual.
- B. If a request for amendment of PHI is accepted, in whole or in part, the record holder must:
 1. Make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment, while preserving the original record.
 2. Timely inform the individual that the PHI amendment is accepted and obtain the individual's identification of, and agreement to have the record holder notify, the relevant persons with which the amendment needs to be shared as set forth below.
 3. Make reasonable efforts to inform and provide the amendment, within a reasonable time, to persons identified by the individual as having received PHI about the individual and needing the amendment; and business associates that the record holder knows may have the PHI that is the subject of the amendment and who may have relied on such information to the detriment of the individual.

C. Denial of Request to Amend Protected Health Information (PHI)

1. An individual's request for amendment of PHI may be denied if the record holder determines that the PHI or record that is the subject of the request:
 - a. Was not created by the record holder, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment.
 - b. Is for information that is not part of the designated record set (the individual's clinical record and billing records).
 - c. Would not be accessible to the individual under section I.B. of this protocol.
 - d. Is accurate and complete.
2. If a request for amendment of PHI is denied, in whole or in part, the record holder must provide the individual with a timely, written denial, written in plain language and containing:
 - a) The basis for the denial.
 - b) The individual's right to submit a written statement disagreeing with the denial and how the individual might file such a statement which will be included in the individual's clinical record.
 - c) A statement that, if the individual does not submit a written statement of disagreement, the individual may request the record holder to include his/her

request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment.

a) A description of how the individual may complain to the record holder, DMHDDAD, the Department of Human Resources (DHR) or to the Secretary of the Department of Health and Human Services (DHHS), including name, or title, and telephone number of the contact office or person designated to receive complaints.

3. The individual may submit to the record holder, DMHDDAD and/or DHR a written statement no more than two (2) pages in length, disagreeing with the denial of all or part of a requested amendment and the basis of such a disagreement.
4. A written rebuttal to the individual's statement of disagreement may be prepared, in which case the record holder must provide a copy to the individual who submitted the statement of disagreement.
5. The record holder must, as appropriate, identify the record or the PHI in the designated record set (the individual's clinical record and billing records) that is the subject of the disputed amendment and append or otherwise link the individual's request for amendment; the denial of the request, the individual's statement of disagreement, if any, and the record holder's rebuttal, if any, to the designated record set. If the individual has submitted a statement of disagreement, the record holder must include the written disagreement with any subsequent disclosure of the PHI to which the disagreement relates.
 - a) When subsequent disclosure described above is made using an electronic transaction that does not permit the additional material to be included, the record holder may separately transmit the material required by the Amending PHI section of this protocol to the recipient of the electronic transaction.
6. If the record holder is notified by another covered entity of an amendment to an individual's PHI, it must amend the designated record set (clinical record and billing record) maintained by the record holder.

D. The titles of persons or offices responsible for receiving and processing requests for PHI amendments must be documented.

E. All documentation related to amending PHI must be retained for a minimum of six (6) years.

V. Tracking Disclosures of Protected Health Information (PHI)

- A. All disclosures of PHI will be tracked by documenting and retaining the accounting of all such disclosures; this documentation should contain the following information:
 1. Date of disclosure.
 2. Name of covered entity or individual who received the information and their address, if known.
 3. Description of the information disclosed.
 4. Purpose of the disclosure (or a copy of the individual's authorization or a copy of a written request for a disclosure for which authorization is not required).
 5. The written accounting provided to an individual requestor.
 6. Titles of persons or offices responsible for receiving and processing requests for accountings of disclosures.
- B. Disclosures for purposes of treatment, payment or health care operations are excluded from the disclosure tracking and accounting requirements. Other excluded disclosures are those made:
 1. Prior to the effective date of the rule (April 14, 2003).

2. To law enforcement officials or correctional institutions who have legal custody of the individual, where the disclosure is for treatment of the individual or the health and safety of other inmates and staff.
 3. To the individual.
 4. For national security or intelligence purposes.
 5. To persons involved in the individual's care.
 6. For notification purposes to the individual's guardian of the person or representative, as defined in the Georgia mental health code, when the disclosure relates to the individual's treatment or payment for treatment.
- C. Individuals can request an accounting of disclosures for a period of up to six (6) years prior to the date of the request; disclosures made prior to April 14, 2003, the compliance date for the Privacy Rule, are excluded from this requirement.
- D. An individual may receive one (1) disclosure accounting in a twelve-month period free-of-charge; a reasonable fee may be charged for more frequent accounting requests.
- E. Individuals must be provided an accounting of disclosures within sixty (60) days of a request; if the record holder cannot provide an accounting of disclosures within the sixty-day period, it must provide information to the requestor as to the reason for the delay and the expected completion date; only one (1) extension is allowed per request.
- F. The record holder may temporarily suspend the right to an accounting to the individual of disclosures for health oversight agencies or law enforcement officials contingent upon submission to the record holder of a statement that indicates an accounting of disclosures will impede an investigation of the individual in question; the statement should include a time-frame for the exclusion period; the statement may be oral, but the exclusion period is then limited to thirty (30) days unless appropriate written documentation is received within that time; although the accounting of disclosure is not being released during this time, the record holder should continue tracking and storing the information for future release.
- G. Recurring disclosures to the same entity or individual that have a regular interval or an authorization with multiple disclosures may have a summary entry; the summary entry requires all of the information as described above for the first disclosure, plus an indication of periodic interval (monthly, weekly, etc.) and the date of the last disclosure.
- H. All documentation related to the tracking of disclosures of PHI must be retained for a minimum of six (6) years.

Georgia Department of Human Resources Division of Mental Health, Developmental Disabilities and Addictive Diseases	PROTOCOL NO: 3.200-02
	ORIGINAL EFFECTIVE DATE:
PROTOCOL SUBJECT: Privacy Rule Administration - Complaints	REVISED EFFECTIVE DATE: N/A
	PAGE 1 OF 41

PROTOCOL

An individual may file a complaint relating to the HIPAA Privacy Rule either directly to the Division (DMHDDAD), to the Department (DHR), or to the Secretary of the Department of Health and Human Services (DHHS). Information on filing a complaint with the Secretary of Health and Human Services is available electronically at www.hhs.gov/ocr/privacyhowtofile.htm. A copy of the HHS complaint form is attached to this protocol as Attachment A. An individual may file a complaint with the Secretary at the following address:

Secretary of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

An individual may file a complaint with the Department of Human Resources at the following address:

DHR Privacy Officer
2 Peachtree Street NW
Room 29.210,
Atlanta, Georgia 30303-3142.

An individual may file a complaint with the DMHDDAD Privacy Coordinator at the following address:

Privacy Coordinator
Division of Mental Health, Developmental Disabilities
and Addictive Diseases
2 Peachtree Street NW
Room 22.240
Atlanta, Georgia 30303-3142.

Upon request, the DMHDDAD Legal and Risk Management Section, Legal Services Officers or DMHDDAD Privacy Coordinator will provide forms and other information about the complaint process necessary to assist an individual wishing to file a complaint. DMHDDAD employees are not authorized to prepare complaints for individuals other than themselves.

- A. Complaints, whether filed directly with the Secretary of DHHS, with DHR, or with DMHDDAD, must be made in writing.
- B. Complaints must name the DHR Division, Office or facility against which the complaint is lodged.
- C. Complaints must describe the acts or omissions upon which the complaint is based.
- D. Complaints filed directly with the Secretary of DHHS must be filed within 180 days of the time the individual became aware, or should have been aware, of the violation.

- E. Complaints may include violations of DHR's and/or DMHDDAD's privacy practices as well as violations of the Privacy Rule itself. Violations may be reported on the "Privacy Violation Report" form, Attachment B of this Protocol.
- F. Individuals may file complaints about the content of DMHDDAD or DHR privacy policies and procedures or other matters governed by the Privacy Rule.
- G. DMHDDAD must receive and document complaints. Although not required by the Privacy Rule, the DMHDDAD Privacy Coordinator will provide a written acknowledgment of receipt of any complaint directed to the Privacy Coordinator within ten (10) days of receipt, provided adequate address information is available to permit the mailing of a written acknowledgment.
- H. All complaints received must be reported by the DMHDDAD Privacy Coordinator to the DHR Legal Services Office within ten (10) days of receipt. A copy of the complaint and the written acknowledgment satisfies this requirement. The complaint may be reported using the "Complaint Report," attached hereto as Attachment C.
- I. DMHDDAD must document complaints and their disposition, if any, and retain the records for six (6) years, or longer according to other applicable authorities, following the disposition or last activity regarding the complaint.
- J. DMHDDAD may not threaten, intimidate, coerce or retaliate against any individual filing a complaint. DMHDDAD may not require an individual to waive his or her rights under the HIPAA Privacy rule as a condition for the provision of treatment, payment, or eligibility for benefits.
- K. If the DMHDDAD denies an individual access to his or her own protected health information (PHI), a written denial must be issued describing how the individual may complain to the Secretary of DHHS and/or to DHR or the Division. The denial must include the name or title and telephone number of the person or office to which complaints may be made.
- L. Though not required by the Privacy Rule, DMHDDAD will make available upon request sample forms and appropriate information to individuals who wish to file complaints with the Secretary or DHR.
- M. The Privacy Coordinator of DMHDDAD may investigate or otherwise respond to complaints and recommend resolution where appropriate. If a violation is discovered as the result of an investigation, it must be reported to the DHR Privacy Officer, (See Attachment B). Complaint resolutions and dispositions must also be reported (See Attachment C).



DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE OF CIVIL RIGHTS (OCR)



HEALTH INFORMATION PRIVACY COMPLAINT

If you have questions about this form, call OCR (toll-free) at:
1-800-368-1019 (any language) or 1-800-537-7697 (TDD)

YOUR FIRST NAME		YOUR LAST NAME	
HOME PHONE ()		WORK PHONE ()	
STREET ADDRESS			CITY
STATE	ZIP	E-MAIL ADDRESS (If available)	

Are you filing this complaint for someone else? ☐ Yes ☐ No

If Yes, whose health information privacy rights do you believe were violated?

FIRST NAME : LAST NAME

Who (or what agency or organization, e.g., provider, health plan) do you believe violated your (or someone else's) health information privacy rights or committed another violation of the Privacy Rule?

PERSON/AGENCY/ORGANIZATION

STREET ADDRESS

CITY

STATE

ZIP

PHONE

()

When do you believe that the violation of health information privacy rights occurred?

LIST DATE(S)

Describe briefly what happened. How and why do you believe your (or someone else's) health information privacy rights were violated, or the privacy rule otherwise was violated? Please be as specific as possible. (Attach additional pages as needed)

Please sign and date this complaint.

SIGNATURE

DATE

Filing a complaint with OCR is voluntary. However, without the information requested above, OCR may be unable to proceed with your complaint. We collect this information under authority of the Privacy Rule issued pursuant to the Health Insurance Portability and Accountability Act of 1996. We will use the information you provide to determine if we have jurisdiction and, if so, how we will process your complaint. Information submitted on this form is treated confidentially and is protected under the provisions of the Privacy Act of 1974. Names or other identifying information about individuals are disclosed when it is necessary for investigation of possible health information privacy violations, for internal systems operations, or for routine uses, which include disclosure of information outside the Department for purposes associated with health information privacy compliance and as permitted by law. It is illegal for a covered entity to intimidate, threaten, coerce, discriminate or retaliate against you for filing this complaint or for taking any other action to enforce your rights under the Privacy Rule. You are not required to use this form. You also may write a letter or submit a complaint electronically with the same information. To submit an electronic complaint, go to our web site at: www.hhs.gov/ocr/privacyhowtofile.html. To mail a complaint see reverse page for OCR Regional addresses.

(The remaining information on this form is optional. Failure to answer these voluntary questions will not affect OCR's decision to process your complaint.)

Do you need special accommodations for us to communicate with you about this complaint (check all that apply)?

- ☐ Braille ☐ Large Print ☐ Cassette tape ☐ Computer diskette ☐ Electronic mail ☐ TDD
- ☐ Sign language interpreter (*specify language*): _____
- ☐ Foreign language interpreter (*specify language*): _____ ☐ Other: _____

If we cannot reach you directly, is there someone we can contact to help us reach you?

FIRST NAME		LAST NAME	
HOME PHONE ()		WORK PHONE ()	
STREET ADDRESS		CITY	
STATE	ZIP	E-MAIL ADDRESS (<i>If available</i>)	

Have you filed your complaint anywhere else? If so, please provide the following. (Attach additional pages as needed.)

PERSON / AGENCY / ORGANIZATION / COURT NAME(S)

DATE(S) FILED	CASE NUMBER(S) (<i>If known</i>)
---------------	------------------------------------

To help us better serve the public, please provide the following information for the person you believe had their health information privacy rights violated (you or the person on whose behalf you are filing).

ETHNICITY (<i>select one</i>)	RACE (<i>select one or more</i>)		
<input type="checkbox"/> Hispanic or Latino	<input type="checkbox"/> American Indian or Alaska Native	<input type="checkbox"/> Asian	<input type="checkbox"/> Native Hawaiian or Other Pacific Islander
<input type="checkbox"/> Not Hispanic or Latino	<input type="checkbox"/> Black or African American	<input type="checkbox"/> White	<input type="checkbox"/> Other (<i>specify</i>): _____
PRIMARY LANGUAGE SPOKEN (<i>if other than English</i>)		HOW DID YOU LEARN ABOUT THE OFFICE FOR CIVIL RIGHTS?	

To mail a complaint, please type or print, and return completed complaint to the
OCR Regional Address based on the region where the alleged discrimination took place.

Region I - CT, ME, MA, NH, RI, VT Office for Civil Rights Department of Health & Human Services JFK Federal Building - Room 1875 Boston, MA 02203 (617) 565-1340; (617) 565-1343 (TDD) (617) 565-3809 FAX	Region V - IL, IN, MI, MN, OH, WI Office for Civil Rights Department of Health & Human Services 233 N. Michigan Ave. - Suite 240 Chicago, IL 60601 (312) 886-2359; (312) 353-5693 (TDD) (312) 886-1807 FAX	Region IX - AZ, CA, HI, NV, AS, GU, The U.S. Affiliated Pacific Island Jurisdictions Office for Civil Rights Department of Health & Human Services 50 United Nations Plaza - Room 322 San Francisco, CA 94102
--	---	--

<p>Region II – NJ, NY, PR, VI</p> <p>Office for Civil Rights</p> <p>Department of Health & Human Services</p> <p>26 Federal Plaza - Suite 3313</p> <p>New York, NY 10278</p> <p>(212) 264-3313; (212) 264-2355 (TDD)</p> <p>(212) 264-3039 FAX</p>	<p>Region VI - AR, LA, NM, OK, TX</p> <p>Office for Civil Rights</p> <p>Department of Health & Human Services</p> <p>1301 Young Street - Suite 1169</p> <p>Dallas, TX 75202</p> <p>(214) 767-4056; (214) 767-8940 (TDD)</p> <p>(214) 767-0432 FAX</p>	<p>(415) 437-8310; (415) 437-8311 (TDD)</p> <p>(415) 437-8329 FAX</p>
<p>Region III - DE, DC, MD, PA, VA, WV</p> <p>Office for Civil Rights</p> <p>Department of Health & Human Services</p> <p>150 S. Independence Mall West - Suite 372</p> <p>Philadelphia, PA 19106-3499</p> <p>(215) 861-4441; (215) 861-4440 (TDD)</p> <p>(215) 861-4431 FAX</p>	<p>Region VII - IA, KS, MO, NE</p> <p>Office for Civil Rights</p> <p>Department of Health & Human Services</p> <p>601 East 12th Street - Room 248</p> <p>Kansas City, MO 64106</p> <p>(816) 426-7278; (816) 426-7065 (TDD)</p> <p>(816) 426-3686 FAX</p>	<p>Region X - AK, ID, OR, WA</p> <p>Office for Civil Rights</p> <p>Department of Health & Human Services</p> <p>2201 Sixth Avenue - Mail Stop RX-11</p> <p>Seattle, WA 98121</p> <p>(206) 615-2290; (206) 615-2296 (TDD)</p> <p>(206) 615-2297 FAX</p>
<p>Region IV - AL, FL, GA, KY, MS, NC, SC, TN</p> <p>Office for Civil Rights</p> <p>Department of Health & Human Services</p> <p>61 Forsyth Street, SW. - Suite 3B70</p> <p>Atlanta, GA 30323</p> <p>(404) 562-7886; (404) 331-2867 (TDD)</p> <p>(404) 562-7881 FAX</p>	<p>Region VIII - CO, MT, ND, SD, UT, WY</p> <p>Office for Civil Rights</p> <p>Department of Health & Human Services</p> <p>1961 Stout Street - Room 1426</p> <p>Denver, CO 80294</p> <p>(303) 844-2024; (303) 844-3439 (TDD)</p> <p>(303) 844-2025 FAX</p>	

Burden Statement

Public reporting burden for the collection of information on this complaint form is estimated to average 45 minutes per response, including the time for reviewing instructions, gathering the data needed and entering and reviewing the information on the completed complaint form. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to: HHS/OS Reports Clearance Officer, Office of Information Resources Management, 200 Independence Ave. S.W., Room 531H, Washington, D.C. 20201.

**PRIVACY VIOLATION REPORT
DEPARTMENT OF HUMAN RESOURCES**

Date:

TO:

Privacy Officer
Department of Human Resources
2 Peachtree Street NW, Room 29.210
Atlanta, GA 30303

THROUGH:

Privacy Coordinator FAX 404/657-6424 or 2173
DMHDDAD
2 Peachtree Street, NW, Room 22.240
Atlanta, GA. 30303

FROM:

Reporter's name

Reporter's title and work unit

Work unit location (Hospital or community provider) Phone No.

Please report potential violations of the HIPAA Privacy Rule using this form.

As required by DHR Privacy Policies, I hereby submit the following information regarding a possible violation of the HIPAA Privacy Rule.

Date of discovery	
Actual occurrence date, if known	
Description of the violation. Attach additional sheets if necessary.	
Violator's name, if known	
Violator's title, if known	
Number of previous similar violations within this work unit	
Number of previous similar violations for this violator	
Describe all actions taken to mitigate any potentially harmful effects of the violation. Attach additional sheets if necessary	
Describe all actions taken to reduce the possibility of recurrence of this violation within this work unit. Attach additional sheets if necessary.	
Has a complaint been received regarding this incident? If so, please attach a copy.	

COMPLAINT REPORT
DEPARTMENT OF HUMAN RESOURCES

Date:

TO:

Privacy Officer
 Department of Human Resources
 2 Peachtree Street NW, Room 29.210
 Atlanta, GA 30303

THROUGH:

Privacy Coordinator
 DMHDDAD
 2 Peachtree Street, NW, Room 22.240
 Atlanta, GA. 30303

FAX 404/657-6424 or 2173

FROM:

Please report Complaints under the HIPAA Privacy Rule using this form.

As required by DHR Privacy Policies, I hereby submit the following information regarding a complaint received under the HIPAA Privacy Rule.

Date received:	
Date acknowledged:	
Basis for the complaint. Attach additional sheets if necessary.	
Is the complaint related to a known violation?	
Complainant's name or identification number.	
Has an investigation been made?	
If yes, summarize findings. Attach additional sheets if necessary.	
Describe actions taken to mitigate any potentially harmful effects of the matter complained of. Attach additional sheets if necessary.	
Describe actions taken to reduce the possibility of recurrence. Attach additional sheets if necessary.	
If resolved, state resolution.	
Complainant notified?	
If yes, notice date.	

Georgia Department of Human Resources Division of Mental Health, Developmental Disabilities and Addictive Diseases	PROTOCOL NO: 3.200-06
PROTOCOL SUBJECT: Sanctions	ORIGINAL EFFECTIVE DATE: 4/14/03
	REVISED EFFECTIVE DATE: N/A
	PAGE 1 OF 2

PROTOCOL

This protocol describes the process for specific sanctions for breaches of confidentiality, violations of the Privacy Rule and/or violations of DMHDDAD's privacy practices, policies, procedures, and protocols. Sanctions which may be imposed by the Division are cumulative of those which may be imposed by statute or regulation.

Specific components and considerations include:

- A. DMHDDAD will establish and apply appropriate sanctions against members of its workforce (employees, volunteers, trainees, or others who come under its direct control), who fail to comply with DHR or DMHDDAD privacy policies, procedures, and protocols, or with requirements relating to the privacy of individually identifiable health information.
- B. DMHDDAD facilities, programs and contracted providers must have written policies, procedures, OR protocols for the application of appropriate sanctions for violations. State hospitals, state operated community programs, and any provider of DMHDDAD services by contract or by memorandum of understanding with DHR, are responsible for ensuring that their policies on sanctions are made known to their employees and agents.
- C. DMHDDAD must document any sanctions that are applied against members of its workforce.
- D. Sanctions do not apply to whistleblowers, provided that
 - a. The workforce member making a disclosure of protected health information (PHI) believes that:
 - 1. The care, services, or conditions provided by DMHDDAD potentially endanger one or more individuals, workers, or the public, OR
 - 2. The workforce member or business associate believes, in good faith, that DMHDDAD has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, AND
 - b. The disclosure of PHI made by the workforce member is to:
 - 1. An appropriate oversight agency, including but not limited to the Long Term Care Ombudsman program, or a public health authority,
 - 2. An appropriate healthcare accreditation organization, or
 - 3. An attorney for the purposes of determining the legal options with regard to the conduct of the workforce member or business associate.
- E. Sanctions do not apply to workforce members who are victims of a criminal act and disclose protected health information (PHI) to a law enforcement official. The disclosed PHI must be about a suspected perpetrator of the criminal act and is limited to the following information:
 - a. Name and address;
 - b. Date and time of treatment.

References: DHR HIPAA Privacy Policies 4.0, 4.1; 45 CFR §§ 164.502(j) and 164.530(e); OCGA §§ 37-3-166, 37-4-125, 37-7-166, and 45-1-4.

<p>Georgia Department of Human Resources Division of Mental Health, Developmental Disabilities and Addictive Diseases</p>	<p>PROTOCOL NO: 3.200-08</p>
	<p>ORIGINAL EFFECTIVE DATE: 4/14/03</p>
<p>PROTOCOL SUBJECT: Business Associates</p>	<p>REVISED EFFECTIVE DATE: N/A</p>
	<p>PAGE 1 OF 3</p>

PROTOCOL

In accordance with Division Policy 3.200 regarding the HIPAA Privacy Rule, the Division and its hospitals and state operated programs and contracted service providers shall identify their business associates.

- A. DMHDDAD shall have an agreement with each business associate. All state-owned or state operated facilities and providers under contract or letter of agreement with the department and/or the division shall also have business associate agreements with entities that perform or assist in performing functions involving the use of individually identifiable health information.
1. DMHDDAD and state-owned or state-operated facilities shall use the business associate terms provided in standard DHR contracts, or the separate business associate agreement issued by the division (see Attachment A) for all such agreements. A copy of all such agreements must be kept on file.
 2. Providers having a contract or letter of agreement with the division will ensure that they have business associate agreement(s) with their agents or subcontractors and that the agreements are HIPAA compliant. The provider must keep a copy of the agreement(s) on file.
 3. Business associate agreements and all documentation relating to the business associate's performance under the Privacy Rule must be retained for as long as the business associate performs or assists in performing functions involving the use of individually identifiable health information, or for six (6) years, whichever is longer.
 4. DMHDDAD shall have access to the business associate agreements of providers upon request.
- B. Disclosures to business associates are subject to minimum necessary requirements. In all cases, DMHDDAD and state-owned or state-operated facilities will ensure that, pursuant to the Official Code of Georgia Annotated, Sections 37-3-166, 37-4-125, and 37-7-166, relating to the treatment of clinical records, the release of clinical records will be conducted as provided by those statutory provisions and by relevant provisions of the HIPAA Privacy Rule. To the extent that any business associate(s) receives such clinical records, the business associate(s) will also adhere to the Georgia Code and the Privacy Rule regarding the treatment and release of such clinical records. Privileged information shall not be released by DMHDDAD or its business associate(s) without proper authorization.
- C. DMHDDAD must inform business associates of the requirement to safeguard PHI and that business associates must provide appropriate training programs for their employees. DMHDDAD may allow business associates access to selected DMHDDAD training materials for these purposes.
- D. Business associates shall be included in policy updates through the Provider manual and through communications from the DHR Privacy Officer and/or the Division Privacy Coordinator. Business associates will be informed of applicable training programs and compliance audits through the Division Training Coordinator, Regional Coordinator, or Privacy Coordinator, as applicable.
- E. If DMHDDAD accepts an amendment to an individual's PHI, the division must make a reasonable effort to inform business associates it knows that have the PHI that is the subject of the amendment and which may have relied on the information to the detriment of the individual. Amendment(s) to PHI will be covered by the procedures outlined in the protocol on individuals' rights.
- F. If DMHDDAD accepts restrictions on the use or disclosure of an individual's PHI, the division's business associates must honor the restrictions.
- G. DMHDDAD state office staff who are responsible for deploying policy and maintaining contracts will keep informed and aware of all business associate relationships and have a mechanism to be notified of changes to those relationships.
- H. DMHDDAD is not considered to have violated Privacy Rule requirements if a business associate disclosed PHI as a whistleblower.
- I. DMHDDAD must mitigate as best it can, any harmful effects from uses and disclosures by its business associates that violate DHR or DMHDDAD privacy policies and procedures.
- J. DMHDDAD must make a good faith effort to obtain satisfactory assurances that each business associate will adhere to Privacy Rule requirements, and if the effort is unsuccessful, document the attempt and the reason such assurance could not be obtained. In such cases, disclosure of PHI may be made to the business associate to the extent necessary to carry out DMHDDAD's legally mandated activities.

- K. DMHDDAD is authorized to terminate any agreement(s) with business associates if the conduct of any business associate(s) constitutes a material breach of the agreement. DMHDDAD will, where feasible, provide an opportunity for the business associate to cure the breach. Where neither termination nor cure is possible, DMHDDAD will report the violation to the Secretary of Health and Human Services.
- L. DMHDDAD will ensure that, upon termination of the agreement with a business associate, protected health information will be returned or destroyed according to the provisions of the contract and in compliance with the HIPAA Privacy Rule.

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement is made and entered into by and between the Georgia Department of Human Resources ("DHR") and the Contractor named below. The parties acknowledge that DHR is "Covered Entity" under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA) and the Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 ("Privacy Rule"). The Privacy Rule requires DHR to obtain satisfactory assurance that Contractor will appropriately safeguard the privacy and provide for the security of Protected Health Information ("PHI") within Contractor's possession, custody or control. Contractor is a Business Associate of DHR as that term is defined under HIPAA and the Privacy Rule. Accordingly, for good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, in order to establish the permitted and required uses and disclosures of PHI, the parties agree as follows:

Contractor will not use or disclose PHI except as permitted or required by this agreement or by law, and when using or disclosing PHI, will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of such use or disclosure. Contractor will establish and use appropriate safeguards to prevent unauthorized use or disclosure of PHI. Contractor will promptly report any unauthorized use or disclosure promptly to DHR, and will ensure that any individual or organization to whom it provides PHI agrees to the same conditions and restrictions with respect to PHI that are applicable to the Contractor. Contractor will allow individuals access to their own PHI, an opportunity to request amendment of such PHI, and all information required to provide an accounting of disclosures of PHI as provided by the Privacy Rule. Contractor will make its internal practices, books and records relating to use or disclosure of PHI to both DHR and the Secretary of Health and Human Services for purposes of determining DHR's compliance with the Privacy Rule. Upon termination of this agreement, Contractor will return all PHI to DHR, retaining no copies of such PHI, and will assure that its agents and subcontractors treat PHI in their possession or control in the same manner. This agreement may be terminated upon notice by DHR if the Contractor violates any material term hereof.

IN WITNESS WHEREOF, DHR and Contractor have caused this Business Associate Agreement to be executed in duplicate on the ____ day of _____, 200__.

GEORGIA DEPARTMENT OF HUMAN RESOURCES

By: _____
Authorized Signature

CONTRACTOR

Typed or Printed Name of Contractor

By: _____
Authorized Signature

GEORGIA DEPARTMENT OF HUMAN RESOURCES Division of Mental Health, Developmental Disabilities and Addictive Diseases	PROTOCOL NO: 3.200-10
	ORIGINAL EFFECTIVE DATE:
PROTOCOL SUBJECT: Disclosure and Authorization for Disclosure of Protected Health Information	REVISED EFFECTIVE DATE: N/A
	PAGE 1 OF 6

PROTOCOL

FY05 Provider Manual, Section V, Chapter V5, 41 Pages

DMHDDAD may disclose protected health information (PHI) of an individual upon the individual's request. DMHDDAD shall have a written authorization from an individual before using or disclosing PHI for any purpose not otherwise permitted by law or allowed by the Privacy Rule.

- A. Authorization forms must be in plain language and must contain the following:
 - 1. Description of the information to be used or disclosed.
 - 2. A description of the purpose of the use or disclosure.
 - 3. Name of the facility or provider authorized to use or disclose the PHI.
 - 4. Name of the receiving person or entity of the use or disclosure.
 - 5. A description of the purpose of the use or disclosure.
 - 6. An expiration date, specified time period, or event triggering expiration.
 - 7. A statement regarding the individual's right to revoke the authorization and a description of how the individual may revoke the authorization.
 - 8. The individual's signature and date of signature.
 - 9. If signed by a parent of a minor, legal custodian of a minor, guardian of the person, or other person legally authorized to sign disclosure of PHI, a description of that person's authority to act for the individual.
 - 10. The signature of a witness and date of signature.
 - 11. A statement that DMHDDAD will not condition treatment, payment, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure.
- B. An authorization is rendered invalid if:
 - 1. The expiration date, specified time period, or event triggering expiration is known to have occurred.
 - 2. The authorization is known by the provider to have been revoked.
 - 3. The authorization has been combined with any other document.
 - 4. The individual's treatment, payment, or health operations are conditioned on signing an authorization.
- C. The facility or provider must give a copy of every fully completed and signed authorization to the person who signed it, and must maintain the original in the individual's clinical record permanently.
- D. The attached form, **Attachment A** "Authorization for Use or Disclosure of Protected Health Information," is required for use by state owned or operated facilities or programs. The facility or program may customize the form to include facility or program letterhead, space for the individual's identification, and the like. No changes in content are permitted without the approval of the Division Privacy Coordinator or the DHR Privacy Officer. If necessary, the authorization may be amended to show that it is valid for the time period necessary to complete the transaction for which the disclosure is made.
- E. Providers of services through contract or letter of agreement may utilize the attached form. Any form utilized by providers must be compliant with the Privacy Rule and the terms of this protocol.
- F. An individual may revoke an authorization at any time, in writing, except to the extent that the entity holding the individual's records has taken action in reliance on the authorization or the authorization was obtained as a condition of obtaining insurance coverage.
- G. An individual who is an adult and who does not have a court-ordered guardian of the person may sign an authorization for disclosure of his/her protected health information. Other persons legally entitled to sign an authorization include:
 - 1. For minor children, a parent, the court-appointed guardian, or a person to whom legal custody of the child has been given by order of a court.
 - 2. For incompetent adults, the court-ordered guardian of the person.
 - 3. For deceased individuals, the legal representative of the individual's estate.
 - 4. For an adult who has signed a durable power of attorney for health care, if the durable power of attorney is in effect at the time, the agent named by the individual.

- H. DMHDDAD may use or disclose protected health information without an individual's written consent or authorization and without giving the individual the opportunity to agree or object in certain circumstances. Such uses and disclosures include the following:
1. When required by law.
 2. AIDS confidential information may be reported or disclosed according to law (OCGA sections 24-9-47; 31-22-9.2).
 3. For public health activities (See OCGA section 31-12-2).
 4. About victims of abuse, neglect, or exploitation (See OCGA section 30-5-4).
 5. For health oversight activities (including audits, investigations, and inspections).
 6. In response to a subpoena or court order from a court of competent jurisdiction, except for privileged matters, and except that substance abuse information may not be disclosed in response to a subpoena, but requires a court order. (OCGA sections 37-3-166, 37-4-125).
 7. A law enforcement officer in the course of a criminal investigation may be informed only:
 - a. whether an individual is or has been a patient in a facility that is not solely a substance abuse facility, as well as the individual's current address, if known, and
 - b. during investigation of a crime on premises of a facility that is not solely a substance abuse facility or against facility personnel or a threat to commit such a crime, a law enforcement officer may be informed as to the circumstances of the incident, including whether the individual allegedly committing or threatening to commit the crime is or has been a patient in the facility, and the name, address, and last known whereabouts of any alleged patient perpetrator.
 8. About deceased persons in response to a valid subpoena from a coroner or medical examiner; to a funeral director in the event the deceased person had an infectious or communicable disease at the time of death, or to the legal representative of the individual's estate (OCGA sections 31-12-2; 31-21-3; 37-3-166, 37-4-125, 37-7-166).
 9. For organ and tissue donation (OCGA section 44-5-143).
 10. For disaster relief purposes (OCGA section 31-12-2).
 11. For the individual's continued treatment (OCGA section 37-3-166, 37-4-125, 37-7-166).
 12. For emergency treatment (OCGA section 37-3-166).
- I. Special rules apply to a disclosure which identifies the individual as a person with a substance abuse diagnosis. The hospital or provider should seek legal and policy review before making any disclosure of substance abuse information without an authorization. Disclosures may not be made unless:
1. The disclosure is for emergency medical care of the individual.
 2. The disclosure is ordered by a court, following a full and fair show cause hearing as described in federal substance abuse confidentiality regulations.
 3. The disclosure is for research activities, audit and evaluation activities, if the party receiving the information has agreed in writing to preserve confidentiality.
 4. Certain information on crimes on program premises or against program personnel.
 5. The disclosure is for reports of suspected child abuse or neglect, as required under state law.
- J. Procedures for Responding to Subpoenas or Discovery Request in a Civil (non-criminal) Case
- a. Protected health information of an individual which does not disclose substance abuse may be produced in response to a subpoena of a court of competent jurisdiction or a Requests for Production of Documents or other discovery request ONLY when EITHER:
 - i. The hospital or provider holding the record receives satisfactory written assurances from the party seeking the protected health information that
 1. the party seeking information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address),
 2. the notice includes sufficient information about the proceeding in which the information is sought to permit the individual to raise an objection to the court, AND
 3. The time for the individual to raise objections to the court has elapsed and no objections were filed, or all objections filed by the individual have been resolved by the court, and the disclosures sought are consistent with such resolution, OR

- ii. the parties to the dispute giving rise to the request have agreed to a qualified protective order and have presented it to the judge, OR the party seeking the information has requested a qualified protective order from the court. A qualified protective order must prohibit the parties to the case from using or disclosing the protected health information for any purpose other than the litigation or proceeding, and must require that the protected health information either be returned to the hospital or provider, or be destroyed at the end of the litigation or proceeding.
 - b. The hospital or provider holding the requested protected health information may, with the assistance of a legal advisor or counsel, undertake to provide the notice and/or obtain the qualified protective order described above. This should generally be done only when there is no reasonable possibility that the party seeking the information will accomplish these requirements.
 - c. If the protected health information which is sought requires a disclosure that the individual has a substance abuse diagnosis (including a health diagnosis that is secondary to or related to substance abuse), the hospital or provider may not follow these procedures. Instead, the requestor must be informed that it is necessary to have either the individual's authorization for use or disclosure of substance abuse information, or a court order based on a full and fair show cause hearing as outlined in the federal regulations on "Confidentiality of Alcohol and Drug Abuse Patient Records" at 42 CFR sections 2.1 and following.
- K. Procedures for Disclosures for Law Enforcement Purposes
A provider may disclose PHI other than substance abuse information in response to a criminal court order or subpoena in a criminal case, provided that the judge issuing the court order or the attorney issuing the subpoena gives assurances that:
 - a. The information sought is relevant and material to a legitimate law enforcement inquiry;
 - b. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
 - c. De-identified information could not reasonably be used.
- L. Redaction or De-Identification of Records
 - a. In the event records are sought by means of a request covered by the Open Records Act of Georgia, the provider must seek legal counsel on whether records may be produced.
 - b. To the extent that any records are required by law to be produced, all identifiers of the individual AND his or her relatives, employers, or household members, must be redacted as follows:
 - i. Name
 - ii. Address
 - iii. Dates relating to the individual, including date of birth, admission and discharge dates, and date of death
 - iv. Age, if over age 89
 - v. Telephone and fax numbers
 - vi. E-mail address
 - vii. Social security number
 - viii. Medical record number
 - ix. Health plan beneficiary number
 - x. Account numbers
 - xi. Driver's License number and other certificate/license numbers
 - xii. Vehicle identifiers and serial numbers, including license plate number
 - xiii. Device identifiers and serial numbers
 - xiv. URLs
 - xv. Internet Protocol (IP) address numbers
 - xvi. Biometric identifiers, including finger and voice prints
 - xvii. Full face photographs and any comparable images identifying the individual
 - xviii. Any other unique number, characteristic (such as physical description, tattoos, or the like).

Authorization for Use or Disclosure of Protected Health Information

I authorize the Georgia Department of Human Resources, Division of Mental Health, Developmental Disabilities and Addictive Diseases provider _____ and its administrative and clinical staff to **(check all that apply)**:

_____ use the following protected health information
_____ disclose the following protected health information to:

The protected health information authorized to be used or disclosed includes:

_____ I authorize the disclosure of alcohol and drug abuse information, if
Initials any.

_____ I authorize the disclosure of any information concerning testing for
Initials HIV (human immunodeficiency virus) and/or treatment for HIV or
AIDS (acquired immune deficiency syndrome) and any related
conditions, if any.

This protected health information is to be used or disclosed for the following purposes:

This authorization shall be in force and effect until EITHER thirty (30) days after I no longer receive services from this Department of Human Resources provider, OR for one year from the date this form is signed, whichever is shorter, OR for the time period necessary to complete transactions required for the purpose above.

I understand that I have the right to revoke this authorization, in writing, at any time by sending such written notification to the Department's Privacy Officer at 2 Peachtree Street NW, Room 29.210, Atlanta, Georgia 30303-3142, OR to the Privacy Coordinator for the Division of Mental Health, Developmental Disabilities, and Addictive Diseases, at 2 Peachtree Street NW, Room 22.240, Atlanta, Georgia 30303-3142 OR to the staff of my service provider.

ATTACHMENT A, 2 PAGES

The Department of Human Resources and its provider will not condition my treatment, payment, or eligibility for any applicable benefits on whether I provide authorization for the requested use or disclosure.

Signature of Individual or Person Legally
Authorized to sign on his/her behalf.

Signature of Witness/Title

Date

Date

Printed Name

Description of Legally Authorized Person's Authority

[Provide a copy of this form to the person granting authorization.]

Use this space only if individual withdraws authorization

Date authorization is withdrawn by individual

Signature of individual

<p style="text-align: center;">GEORGIA DEPARTMENT OF HUMAN RESOURCES Division of Mental Health, Developmental Disabilities and Addictive Diseases</p>	<p style="text-align: center;">PROTOCOL NO: 3.200-14</p>
	<p>ORIGINAL EFFECTIVE DATE:</p>
<p>PROTOCOL SUBJECT: Notice of Privacy Practices</p>	<p>REVISED EFFECTIVE DATE: N/A</p>
	<p>PAGE 1 OF 4</p>

PROTOCOL

All consumers are entitled to written notice of the privacy practices of the Division of Mental Health, Developmental Disabilities, and Addictive Diseases.

- (a) DMHDDAD will promptly seek authorization from the Department of Human Resources to revise and re-distribute the Notice of Privacy Practices whenever there is a material change to uses and disclosures, the individual's rights, DMHDDAD's legal duties, or other privacy practices stated in the Notice.
- (b) The Notice must be in plain language and include:
 - 1) Information regarding uses and disclosures of PHI
 - 2) Statement of an individual's privacy rights regarding protected health information
 - 3) DMHDDAD's responsibilities under the Privacy Rule
 - 4) How to file complaints with the service provider, DMHDDAD, or the Secretary of DHHS

FY05 Provider Manual, Section V, Chapter V6, 41 Pages

- 5) Name, title and phone number of the designated contact for more information on DMHDDAD's privacy practices
- 6) Effective date of the notice
- (c) The Notice, **Attachment A**, must be used, without alteration, by DMHDDAD state-owned or state-operated facilities. As the use or disclosure of protected health information changes, the Department may revise the Notice and copies of the revised Notice will be posted and promptly distributed to division staff, regional offices, state-owned or state-operated facilities, providers, and consumers. Notice must be provided to individuals within 60 days of a material revision to the notice.
- (d) Providers operating under contract or memorandum of understanding with DHR or the Division must utilize a notice of privacy practices that complies with the HIPAA Privacy Rule.
- (e) Individuals must be notified every 3 years of the availability of the Notice and how to obtain it. Providing the Notice electronically satisfies the privacy practices notice requirement.
- (f) In order to preserve the opportunity to raise questions about DMHDDAD's privacy policies, DMHDDAD direct treatment providers must make good faith efforts to obtain a written acknowledgment of receipt of the notice of privacy practices. This acknowledgment may be made by the individual, parent (for minor individuals) or guardian of the person of an individual. In the event the individual, parent, or guardian declines to provide such an acknowledgment, the effort to obtain it should be documented. A copy of the notice (signed if possible) will be kept in the individual's clinical record.
- (g) DMHDDAD will ensure that a copy of the notice is provided to individuals, parents of minor individuals, and guardians of individuals inquiring about or applying for services through DMHDDAD.
- (h) Every individual, or his/her parent or guardian if applicable, is entitled to a copy of the notice upon request.
- (i) Facilities, providers of services and regional offices must ensure that the Notice of Privacy Practices is posted at all times in a prominent location where it is reasonable to expect individuals who are seeking or receiving services to be able to read the notice. Additional copies must be available for distribution upon request.

Notice of Privacy Practices
Georgia Department of Human Resources
Division of Mental Health, Developmental Disabilities and Addictive Diseases

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED BY THE DEPARTMENT AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY. This notice is effective April 14, 2003. It is provided to you pursuant to provisions of the Health Insurance Portability and Accountability Act of 1996 and related federal regulations. If you have questions about this Notice please contact the Department's Privacy Officer or Division's Privacy Coordinator at the address below.

The Department of Human Resources is an agency of the State of Georgia responsible for numerous programs which deal with medical and other confidential information. Both federal and state laws establish strict requirements for most programs regarding the disclosure of confidential information, and the Department must comply with those laws. For situations where stricter disclosure requirements do not apply, this Notice of Privacy Practices describes how the Department may use and disclose your protected health information for treatment, payment, health care operations and for certain other purposes. This notice also describes your rights to access and control your protected health information, and provides information about your right to make a complaint if you believe the Department has improperly used or disclosed your "protected health information." Protected health information is information that may personally identify you and relates to your past, present or future physical or mental health or condition and related health care services. The Department is required to abide by the terms of this Notice of Privacy Practices, and may change the terms of this notice, at any time. A new notice will be effective for all protected health information that the Department maintains at the time of issuance. Upon request, the Department will provide you with a revised Notice of Privacy Practices by posting copies at its facilities, publication on the Department's website, in response to a telephone or facsimile request to the Privacy Office, or in person at any facility where you receive services from the Department.

1. Uses and Disclosures of Protected Health Information Your protected health information may be used and disclosed by the Department, its administrative and clinical staff and others involved in your care and treatment for the purpose of providing health care services to you, and to assist in obtaining payment of your health care bills.

a. Treatment: Your protected health information may be used to provide, coordinate, or manage your health care and any related services, including coordination of your health care with a third party that has your permission to have access to your protected health information, such as, for example, a health care professional who may be treating you, or to another health care provider such as a specialist or laboratory.

b. Payment: Your protected health information may be used to obtain payment for your health care services. For example, this may include activities that a health insurance plan requires before it approves or pays for health care services such as: making a determination of eligibility or coverage, reviewing services provided to you for medical necessity, and undertaking utilization review activities.

c. Health Care Operations: The Department may use or disclose your protected health information to support the business activities of the Department, including, for example, but not limited to, quality assessment activities, employee review activities, training, licensing, and other business activities. Your protected health information may be used to contact you about appointments or for other operational reasons. Your protected health information may be shared with third party "business associates" who perform various activities that assist us in the provision of your services.

2. Other Permitted or Required Uses and Disclosures with Your Authorization or Opportunity to Object

Other uses and disclosures of your protected health information will be made only with your written

authorization, which you may revoke at any time, except as permitted or required by law as described

below. Generally, if there is protected health information which identifies you as a person who has applied

for or received substance abuse services, that information will not be disclosed without your consent unless the law allows or requires such a disclosure. The Department may use and disclose your protected health information when you authorize in writing such use or disclosure of all or part of your protected health information. If you are hospitalized, the Department may use and disclose certain protected health information to your representative, as that term is defined in the Georgia Mental Health Code, upon your admission or discharge; you may be given a chance to object to certain other disclosures to your representative.

3. Permitted or Required Uses and Disclosures without Your Authorization or Opportunity to Object

The Department may use or disclose your protected health information without your authorization for continuity of your care or for your treatment in an emergency or when clinically required; when required to do so by law; for public health purposes; to a person who may be at risk of contracting a communicable disease; to a health oversight agency; to an authority authorized to receive reports of abuse or neglect; in certain legal proceedings; and for certain law enforcement purposes. Protected health information may also be disclosed without your authorization to a coroner or medical examiner, and to the legal representative of your estate.

4. Required Uses and Disclosures: Under the law, the Department must make disclosures to you and when required by the Secretary of the Department of Health and Human Services to investigate or determine the Department's compliance with the requirements of the Privacy Rule at 45 CFR Sections 164.500 et. seq.

5. Your Rights The following is a statement of your rights with respect to your protected health information and a brief description of how you may exercise these rights.

a. You have the right to inspect and copy your protected health information. You may inspect and obtain a copy of protected health information about you for as long as the Department maintains the protected health information. This information includes medical and billing records and other records the Department uses for making medical and other decisions about you. A reasonable, cost-based fee for copying, postage and labor expense may apply. Under federal law you may not inspect or copy psychotherapy notes; information compiled in anticipation of, or for use in, a civil, criminal, or administrative proceeding, or protected health information that is subject to a federal or state law prohibiting access to such information.

b. You have the right to request restriction of your protected health information. You may ask the Department not to use or disclose any part of your protected health information for the purposes of treatment, payment or healthcare operations, and not to disclose protected health information to family members or friends who may be involved in your care. Such a request must state the specific restriction requested and to whom you want the restriction to apply. The Department is not required to agree to a restriction you request, and if the Department believes it is in your best interest to permit use and disclosure of your protected health information, your protected health information will not be restricted, except as required by law. If the Department does agree to the requested restriction, the Department may not use or disclose your protected health information in violation of that restriction unless it is needed to provide emergency treatment.

c. You have the right to request to receive confidential communications from us by alternative means or at an alternative location. Upon written request to a person listed in section 6 below, the Department will accommodate reasonable requests for alternative means for the communication of confidential information, but may condition this accommodation upon your provision of an alternative address or other method of contact. The Department will not request an explanation from you as to the basis for the request.

d. You may have the right to request amendment of your protected health information. If the Department created your protected health information, you may request an amendment of that information for as long as it is maintained by the Department. The Department may deny your request for an amendment, and if it does so will provide information as to any further rights you may have with respect to such denial. Please contact one of the persons listed in section 6 below if you have questions about amending your medical information.

e. You have the right to receive an accounting of certain disclosures the Department has made of your protected health information. This right applies only to disclosures for purposes other than treatment, payment or healthcare operations, excluding any disclosures the Department made to you, to family members or friends involved in your care, or for national security, intelligence or notification purposes. You have the right to receive legally specified information regarding disclosures occurring after April 14, 2003, subject to certain exceptions, restrictions and limitations.

f. You have the right to obtain a paper copy of this notice from the Department, upon request.

6. Complaints You may complain to us and to the United States Secretary of Health and Human Services if you believe your privacy rights have been violated. You may file a complaint in writing with the DHR Facility which maintains your protected health information at telephone_____, facsimile_____, or by mail to _____. You must state the basis for your complaint. The Department will not retaliate against you for filing a complaint. You may also contact the **Division's Privacy Coordinator by telephone at (404) 657-6423, facsimile (404) 657-6424, or by mail to 2 Peachtree Street NW, Room 22.240, Atlanta, Georgia 30303-3142,** for further information about the complaint process or this notice.

Please sign a copy of this Notice of Privacy Practices for the Department's records.

I have received a copy of this Notice on the date indicated below.

Signature of Individual or Legally Authorized Person

Date